

## FACT SHEET

# Uncover your hidden attack surface with the Attack Surface Detector (ASD) plugin for OWASP ZAP 🕥 and Burp Suite 💕

Jse Attack Surface Detector to analyze These results may include URL endpoint				inceers and impore them inc	o baip.					
			iy not nna.							
Import Endpoints from Source Im	port Endpoints from	CLI JSON								
otal Endpoints Detected: 83										
Detected Endpoints Number of Detected Parameters /asvnc/callable/response-body 0			GET Method POST Metho			d New/Modified				
	0				_	1			4	<u>^</u>
	0				_	1			-	
	0					1			8	
	0			ñ	-	1				
	0			i .	_	i				
	0			Ĩ.		í			ă	
form	8				I				3	
/mapping/p	Ă					s			_	
views/*/pat/localhost:8080	A	Contents								
data/pararing-mvc-showcase		Host	Meth	LIBI	Para	Status	Length	MIME type	Title	Comment
data/groupasync									THEIG	
Callable		http://localho		/spring-mvc-showc		200	179	text		New endpoint de
data/stand	andling	http://localho		/spring-mvc-showc		200	170	text		New endpoint de
data/(nath C exception		http://localho		/spring-mvc-showc		200	200	text		Modified endpoir
fileupload D response-body		http://localho		/spring-mvc-showc	$\checkmark$	200	1855	HTML	fileup	Modified endpoir
fileupload 🗋 view			st:80 POST	/spring-mvc-showc	$\checkmark$	403	1360	HTML	Apac	Modified endpoir
deferred recult		http://localho	st:80 POST	/spring-mvc-showc	$\checkmark$	403	1360	HTML	Apac	Modified endpoir
elected E		http://localho	st:80 GET	/spring-mvc-showc		200	256	text		Endpoint detect
NL: Description of a factor		http://localho	st:80 GET	/spring-mvc-showc		200	182	text		Endpoint detect
orm model-and-view		http://localho		/spring-mvc-showc		200	432	HTML	My H	Endpoint detect
lethods:		http://localho		/spring-mvc-showc		200	206	text		Endpoint detect
OST class-mapping		http://localho		/spring-mvc-showc		200	424	HTML	My H	Endpoint detect
arameters		http://localho		/spring-mvc-showc		200	182	text	my ma	Endpoint detect
iquiry - Stri 🦰 🔔						200	196			Endpoint detect
hone - INT 🌼 consumes		http://localho		/spring-mvc-showc				text		
iquiryDetail 🔀		http://localho		/spring-mvc-showc		200	185	text		Endpoint detect
ame Strin 🗋 header		http://localho		/spring-mvc-showc	<b>V</b>	200	192	JSON		Endpoint detect
urrency - St		http://localho		/spring-mvc-showc		200	189	text		Endpoint detect
ercent - St 🗋 notheader		http://localho		/spring-mvc-showc		200	206	text		Endpoint detect
rthDate - 9 🗋 parameter		http://localho		/spring-mvc-showc		200	246	text		Endpoint detect
e-INTEGE D path		http://localho		/spring-mvc-showc		200	197	text		Endpoint detect
🕫 📴 path		http://localho	st:80 GET	/spring-mvc-showc	$\checkmark$	200	211	text		Endpoint detect
N *		http://localho		/spring-mvc-showc		200	209	text		Endpoint detect
D produces		http://localho		/spring-mvc-showc		200	272	text		Endpoint detect
convert		http://localho		/spring-mvc-showc		200	231	text		Endpoint detect
bean		http://localho		/spring-mvc-showc		200	162	text		Endpoint detect
collection		http://localho		/spring-mvc-showc		200	154	text		Endpoint detect
		http://localho		/spring-mvc-showc		200	328	text		Endpoint detect
🖸 values=-1										
custom		http://localho	st:80 GET	/spring-mvc-showc		200	197	text		Endpoint dete

Automated penetration tests are a popular and effective method to identify exploitable vulnerabilities for an application, but often suffer capability gaps that are difficult to overcome with current tools. The most significant problem is that an application's attack surface is often not fully enumerated prior to testing, and consequently part of that attack surface goes unexercised. Currently, unlinked endpoints must be identified by manual code review, which is a time-consuming—and therefore expensive—process.

The Attack Surface Detector, under the ASTAM program, consists of a pair of plugins for widely adopted DAST tools, Portswigger's Burp Suite and OWASP ZAP (Zed Attack Proxy). These plugins will automatically examine the application's source code via static analysis, finding hidden or unlinked endpoints in the process, and further identifying their optional parameters and data types, which most DAST scans will miss. This greatly broadens the visible, testable portions of the application's attack surface, providing the basis for more thorough penetration testing. This newly enumerated surface can then be spidered and tested with Burp Suite or OWASP ZAP, or manually pen-tested.

## About

Attack Surface Detector was developed under the DHS S&T ASTAM contract #HHSP233201600058C. It is available with the download links on the right and at: https://github.com/secdec/







## **KEY FEATURES**

- Identifying of unlinked endpoints
- Uncovering optional parameters
- Uncovering parameter datatypes and names

• Leveraging attack surface difference generator to highlight differences between selected versions of your application

• Automatically generating HTTP requests based on metadata discovered during hybrid analysis

• Leveraging Burp and ZAP pen testing tools using ASD identified endpoints and parameters within a common testing environment

• Ability to import endpoints from the ASD command line interface (CLI) tool output, eliminating the need to provide direct access to source code

## **KEY BENEFITS**

• Identify attack surface gaps – fills in gaps in the visible attack surface by locating unlinked endpoints that go unobserved during traditional spidering and brute force testing efforts

• Enhanced parameter detection – identifies optional parameters that could go unnoticed which may open back door vulnerabilities in your applications

• **Reduced effort and costs** – reduced manual efforts to detect attack surface gaps and optional parameters saves time and money

• Focus of penetration testing on newly identified attack surfaces

• Easy installation – available as an open source project through GitHub, the OWASP ZAP Marketplace and coming soon to the PortSwigger BApp Store

#### SUPPORTED FRAMEWORKS

Struts Django Ruby on Rails ASP.NET Web Forms JSP/Java Servlets ASP.NET MVC Spring MVC

#### **FUTURE ENDEAVORS**

- PHP support is being added through community collaboration
- Process multiple frameworks for the same project
- Integration of ASD into more automated pen testing pipelines

## **DOWNLOAD LINKS**

https://github.com/secdec/attack-surface-detector-zap

https://github.com/secdec/attack-surface-detector-burp

https://github.com/secdec/attack-surface-detector-cli

https://www.owasp.org/index.php/OWASP\_Attack\_Surface\_Detector\_ Project

6 Bayview Avenue, Northport, NY 11768 (631) 759-3988 • info@securedecisions.com